EXHIBIT 16

Automotive News

December 04, 2006 12:00 AM

Dealer security stirs insecurity

Vendors wary of Reynolds plan for computer systems

Ralph Kisiel

The Reynolds and Reynolds Co. wants to make it tougher for outsiders to tap into data from dealership computer systems without the proper connections. The effort is creating controversy and debate among dealers and third-party vendors such as AutoTrader.com that depend on access to dealer data.

ACCESS DENIED

Reynolds is tightening dealer management system security to
- Protect dealer data from inappropriate use by third-party vendors
- Comply with state and federal privacy and consumer-data laws
- Decrease chances for unauthorized data access or loss
- Keep Reynolds' ERA system performing optimally

Source: Reynolds and Reynolds Co.

The Reynolds and Reynolds Co. wants to make it tougher for outsiders to tap into data from dealership computer systems without the proper connections.

The effort is creating controversy and debate among dealers and third-party vendors such as AutoTrader.com that depend on access to dealer data. Reynolds, now under new ownership, stands by its efforts to beef up security measures.

Reynolds has been slowly adding security patches since June 2005 and monitoring dealership systems to identify what parties are accessing the systems through what are known as unsupported interfaces.

The move has caught the attention of the National Automobile Dealers Association.

Members of NADA's information technology committee will meet with Reynolds Vice Chairman Fin O'Neill on Friday, Dec. 8, to discuss the new security measures and other implications of the recent Universal Computer Systems Inc. acquisition of Reynolds. The companies are merging operations.

"We're going to try to discuss this with them because it affects 11,000 dealers," says Bill Keith, head of NADA's IT committee and dealer principal at Freehold Ford in Freehold, N.J. It appears Reynolds is taking on UCS' closed approach to third-party access, he says.

Echoes of the parent

"First, how much of a handicap is it going to be, because we all have needs to have customer follow-up systems and other third-party services," Keith says.

He acknowledges that security of dealer data is critical.

"But dealers have been doing this forever, and no one's going in and stealing stuff - it's just not happening," Keith says. Scores of software vendors provide services to dealers by tapping into the Reynolds system through an unsupported, or hostile, interface.

For example, a dealership might contract with a third-party vendor to send service reminders to dealership customers. That vendor needs to pull customer-service histories from the dealership's computer system.

Another vendor might maintain the dealership's online inventory, pulling data nightly from the store's computer system.

"We believe the only way we can meet our customers' needs for openness, safety and security is through more actively managing and supporting the access to the system," Paul Whitworth, Reynolds' vice president of information services, told Automotive News.

During the first half of this year, Reynolds investigated more than 100 incidents in which third-party vendors accessed data through an unsupported interface and corrupted the dealership's database, Whitworth says. "Sometimes we can get that fixed in an hour," he says. "But we had one incident which took nine days."

Reynolds and its chief rival, ADP Dealer Services, offer third-party vendors alternatives to unsupported interfaces. Reynolds, for example, has developed certified interfaces with J.D. Power and Associates' Power Information Network, Enterprise Rent-A-Car Co. and Stronghold Technologies Inc. But the rigorous Reynolds certification process can cost $10,000 to $20,000.

The software patches will protect data from inappropriate use by third-party vendors, assist in compliance with state and federal legislation, decrease the likelihood of unauthorized data access or loss, and keep the Reynolds system performing optimally, says Robert Schaefer, Rey-nolds' director of data services.

Reynolds now has the largest share of the dealership management system market in the United States. It wants to lead the industry in tightening security of dealership systems,

Whitworth says. UCS has long been known for having a closed system that prevents unauthorized third-party access.

Opposition organizes

The third-party companies that make their business moving data in and out of dealership systems are alarmed about losing access. Eight companies earlier this year formed a coalition, Open Secure Access Inc., to protect their access to data. They are Autobytel, AutoTrader, Carfax, Cars.com, CarsDirect, Cobalt Group, DealerTrack Inc. and JMsolutions. Kelley Blue Book Co. Inc. and RouteOne LLC joined the founding members last week.

"There's a whole lot of good reasons for all those applications to be out there," says Allan Stejskal, president of Open Secure Access. Stejskal says he understands the need for tightened security and for Reynolds to have control over its computing environment.

"But who should decide who's coming in to the system - is it Reynolds or is it the dealer?" Stejskal says. "I think the dealer's in the best position to evaluate the risks and benefits of having a third party coming in or out of their system."

ADP Dealer Services continually enhances the security of its dealership management system but will not charge dealers or third-party vendors to access the ADP system, says Kevin Henahan, senior vice president of marketing.

"We don't tell the dealer, if someone wants access to their data, they have to come to ADP to gain access to the data," Henahan says. "It's ultimately the dealer's data. If he wants to give that data to somebody, for us to try to charge a toll doesn't seem like the right thing to do. So we're not going to go down this path."

You may e-mail Ralph Kisiel at ***rkisiel@crain.com***

Source URL: *https://www.autonews.com/article/20061204/SUB/61201031/dealer-security-stirs-insecurity*